

Docket No.: 1509-493

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Katsuyuki YUMOTO

Serial No.: NEW

Filed: April 9, 2004

For: ACCESS CONTROL SYSTEM AND METHOD

CLAIM OF PRIORITY AND SUBMISSION OF PRIORITY DOCUMENT

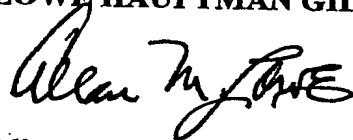
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 35 U.S.C. §119, Applicant hereby claims the foreign priority benefit of Japanese Patent Application No. 2003-104756, filed April 9, 2003. A certified copy of the priority document is attached.

Respectfully submitted,

LOWE HAUPTMAN GILMAN & BERNER, LLP



Allan M. Lowe, Registration No. 19,641

1700 Diagonal Road, Suite 310
Alexandria, VA 22314
(703) 684-1111 Telephone
(703) 518-5499 Telecopier

Date: April 9, 2004

AML:rk



日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 4月 9日
Date of Application:

出願番号 特願2003-104756
Application Number:

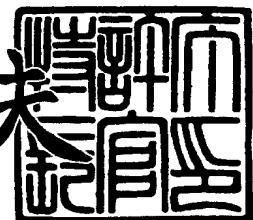
[ST. 10/C] : [JP2003-104756]

出願人 日本ヒューレット・パッカード株式会社
Applicant(s):

2004年 3月 22日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 200310074

【提出日】 平成15年 4月 9日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/00

【発明者】

【住所又は居所】 東京都杉並区高井戸東3丁目29番21号 日本ヒューレット・パッカード株式会社内

【氏名】 湯本 勝之

【特許出願人】

【識別番号】 399117110

【氏名又は名称】 日本ヒューレット・パッカード株式会社

【代理人】

【識別番号】 110000039

【氏名又は名称】 特許業務法人 アイ・ピー・エス

【代表者】 早川 明

【電話番号】 045-228-0131

【手数料の表示】

【予納台帳番号】 132839

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要



【書類名】 明細書

【発明の名称】 アクセス制御システムおよびその方法

【特許請求の範囲】

【請求項 1】

オペレーティングシステムと、

前記オペレーティングシステムにより実行される1つ以上のプロセスそれぞれによる1つ以上のデバイスそれぞれに対するアクセスを制御するアクセス制御装置と

を含むアクセス制御システムであって、

前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれを介して、前記デバイスそれぞれにアクセスし、

任意の前記デバイスそれぞれに対応して、複数のデバイスファイルが生成されることがあり、

前記オペレーティングシステムは、

前記プロセスそれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して、前記デバイスファイルそれを生成するデバイスファイル生成手段と、

前記経路それぞれに対して、前記デバイスファイルそれぞれにアクセスする方法を示すアクセス規則を設定するアクセス規則設定手段と、

前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御するアクセス制御手段と

を有し、

前記アクセス制御装置は、同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を統一し、

前記アクセス制御手段は、前記アクセス規則が統一されたときには、前記統一されたアクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御する

アクセス制御システム。

【請求項 2】

1つ以上のプロセスそれぞれによる1つ以上のデバイスそれぞれに対するアクセスを制御するアクセス制御装置であって、

前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれぞれを介して、前記デバイスそれぞれにアクセスし、

前記デバイスファイルそれぞれは、前記プロセスそれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して生成され、

前記経路それぞれに対して、前記デバイスファイルそれぞれにアクセスする方法を示すアクセス規則が設定され、

前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスが制御され、

任意の前記デバイスそれぞれに対応して、複数のデバイスファイルが生成されることがあります、

同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出するアクセス規則抽出手段と、

前記抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出するアクセス規則導出手段と

を有するアクセス制御装置。

【請求項3】

前記アクセス規則導出手段は、前記デバイスごとに抽出された複数のアクセス規則が異なるときに、これら複数のアクセス規則のいずれかを、前記統一されたアクセス規則として導出する

請求項2に記載のアクセス制御装置。

【請求項4】

前記アクセス規則導出手段は、前記デバイスごとに抽出された複数のアクセス規則が異なるときに、前記デバイスファイルとリンクされたファイルの属性に基づいて、前記統一されたアクセス規則を導出する

請求項2に記載のアクセス制御装置

【請求項5】

前記アクセス規則導出手段は、前記デバイスごとに抽出された複数のアクセス

規則が異なっているときに、これら複数のアクセス規則の内、前記デバイスファイルへのアクセスに対する制限が多いいいずれかを、前記統一されたアクセス規則として導出する

請求項 2 に記載のアクセス制御装置

【請求項 6】

前記プロセスはオペレーティングシステムにより実行され、

前記経路は、前記オペレーティングシステムが管理する 1 つ以上のディレクトリに存在し、前記プロセスそれぞれと前記デバイスファイルそれぞれとの間でリンクされた 1 個以上のファイルにより構成され、

前記アクセス規則は、前記デバイスファイルとリンクされたファイルが存在するディレクトリそれぞれに対して設定される

請求項 2 ～ 5 のいずれかに記載のアクセス制御装置。

【請求項 7】

前記アクセス規則は、少なくとも、前記デバイスファイルにリンクされたファイルそれぞれが、前記デバイスファイルそれぞれに対する読み出しおよび書き込みそれぞれが許可されるか否かを示す

請求項 2 ～ 6 のいずれかに記載のアクセス制御装置。

【請求項 8】

前記オペレーティングシステムは、前記アクセス規則を記憶し、

前記アクセス規則抽出手段は、前記オペレーティングシステムが起動されたときに、前記記憶されたアクセス規則から、同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出し、

前記アクセス規則導出手段は、前記オペレーティングシステムが起動されたときに抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出する

請求項 2 ～ 7 のいずれかに記載のアクセス制御装置。

【請求項 9】

前記オペレーティングシステムは、前記アクセス規則の変更を受け入れ、前記変更されたアクセス規則を、前記アクセス制御装置に通知し、

前記アクセス規則抽出手段は、前記アクセス規則の変更が通知されたときに、前記変更されたアクセス規則と関係する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出し、

前記アクセス規則導出手段は、前記アクセス規則の変更が通知されたときに抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出する

請求項2～8のいずれかに記載のアクセス制御装置。

【請求項10】

1つ以上のプロセスそれぞれによる1つ以上のデバイスそれぞれに対するアクセスを制御するアクセス制御方法であって、

前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれぞれを介して、前記デバイスそれぞれにアクセスし、

前記デバイスファイルそれぞれは、前記プロセスそれぞれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して生成され、前記デバイスファイルは、任意の前記デバイスそれぞれに対応して、複数、生成されることがあり、

前記経路それぞれに対して、前記デバイスファイルそれぞれにアクセスする方法を示すアクセス規則が設定され、

同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出し、

前記抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出し、

前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御する

アクセス制御方法。

【請求項11】

1つ以上のプロセスそれぞれによる1つ以上のデバイスそれぞれに対するアクセスを制御するプログラムであって、

前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれぞれを介して、前記デバイスそれぞれにアクセスし、

前記デバイスファイルそれぞれを、前記プロセスそれぞれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して生成するステップであって、前記デバイスファイルは、任意の前記デバイスそれぞれに対応して、複数、生成されることがあるステップと、

前記経路それぞれに対して、前記デバイスファイルそれぞれにアクセスする方法を示すアクセス規則を設定するステップと、

前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御するステップと、

同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出するステップと、

前記抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出するステップと

をコンピュータに実行させるプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンピュータのデバイスに対するアクセスを制御するアクセス制御システムおよびその方法に関する。

【0002】

【従来の技術】

コンピュータのオペレーティングシステム（OS）として、UNIX（登録商標）が一般的に用いられている。

また、近年、このUNIX（登録商標）をパーソナルコンピュータ向けにしたLINUXが普及している。

また、例えば、非特許文献1は、これらのOSの脆弱性を手当てる方法を開示する。

【0003】

【非特許文献1】 "Compartmented mode operating system"（情報処理学会・第65回（平成15年（2003年））全国大会講演論文集（5）・セクショ

ン 2 T 9 - 4 / 5 - 5 5 5 ページ)

【0004】

【発明が解決しようとする課題】

本発明は、上述した背景からなされたものであり、コンピュータのOSの脆弱性を手当てして、その安全性を向上させることができるアクセス制御システムおよびその方法を提供することを目的とする。

【0005】

【課題を解決するための手段】

【アクセス制御システム】

上記目的を達成するために、本発明に係るアクセス制御システムは、オペレーティングシステムと、前記オペレーティングシステムにより実行される1つ以上のプロセスそれぞれによる1つ以上のデバイスそれぞれに対するアクセスを制御するアクセス制御装置とを含むアクセス制御システムであって、前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれぞれを介して、前記デバイスそれぞれにアクセスし、任意の前記デバイスそれぞれに対応して、複数のデバイスファイルが生成されることがあり、前記オペレーティングシステムは、前記プロセスそれぞれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して、前記デバイスファイルそれぞれを生成するデバイスファイル生成手段と、前記経路それぞれに対して、前記デバイスファイルそれぞれにアクセスする方法を示すアクセス規則を設定するアクセス規則設定手段と、前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御するアクセス制御手段とを有し、前記アクセス制御装置は、同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を統一し、前記アクセス制御手段は、前記アクセス規則が統一されたときには、前記統一されたアクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御する。

【0006】

【アクセス制御装置】

また、本発明に係るアクセス制御装置は、1つ以上のプロセスそれぞれによる

1つ以上のデバイスそれぞれに対するアクセスを制御するアクセス制御装置であって、前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれぞれを介して、前記デバイスそれぞれにアクセスし、前記デバイスファイルそれぞれは、前記プロセスそれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して生成され、前記経路それぞれに対して、前記デバイスファイルそれにアクセスする方法を示すアクセス規則が設定され、前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスが制御され、任意の前記デバイスそれぞれに対応して、複数のデバイスファイルが生成されることがあり、同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出するアクセス規則抽出手段と、

前記抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出するアクセス規則導出手段とを有する。

【0007】

[アクセス制御方法]

また、本発明に係るアクセス制御方法は、1つ以上のプロセスそれぞれによる1つ以上のデバイスそれぞれに対するアクセスを制御するアクセス制御方法であって、前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれぞれを介して、前記デバイスそれぞれにアクセスし、前記デバイスファイルそれぞれは、前記プロセスそれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して生成され、前記デバイスファイルは、任意の前記デバイスそれぞれに対応して、複数、生成されることがあり、前記経路それぞれに対して、前記デバイスファイルそれにアクセスする方法を示すアクセス規則が設定され、同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出し、前記抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出し、前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御する。

【0008】

[プログラム]

また、本発明に係るプログラムは、1つ以上のプロセスそれぞれによる1つ以

上のデバイスそれぞれに対するアクセスを制御するプログラムであって、前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれぞれを介して、前記デバイスそれぞれにアクセスし、前記デバイスファイルそれぞれを、前記プロセスそれぞれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して生成するステップであって、前記デバイスファイルは、任意の前記デバイスそれぞれに対して、複数、生成されることがあるステップと、前記経路それぞれに対して、前記デバイスファイルそれぞれにアクセスする方法を示すアクセス規則を設定するステップと、前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御するステップと、同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出するステップと、前記抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出するステップとをコンピュータに実行させる。

【0009】

【発明の実施の形態】

[本発明の背景]

まず、実施形態の説明に先立って、その理解を助けるために、本発明にかかるアクセス制御方法がなされるに至った背景、および、本発明に係るアクセス制御方法の概要を説明する。

【0010】

[デバイスへのアクセスの際に生じる問題]

図1は、本発明の背景を、具体例を挙げて説明する図である。

例えば、上述したUNIX（登録商標）やLINUXなどと同様な処理を行うOSにおいては、実行中のプロセスが、コンピュータの記憶装置、インターフェースおよび出力装置などの資源（以下、「デバイス」とも記す）にアクセスするために、デバイスそれぞれに対応して設けられるデバイスファイル実体（以下、「デバイスファイル」とも記す）が用いられる。

【0011】

つまり、例えば、図1に示すように、実行中のプロセスは、ディレクトリ”a／b”の中の”file#1”を介して、”file#1”にリンクされたデバ

イスファイルにアクセスすることにより、デバイスへのアクセスを行う。

また、図1に同様に例示するように、実行中のプロセスは、ディレクトリ”a／c”の中の”file#2”を介して、”file#2”にリンクされたデバイスファイルにアクセスすることにより、デバイスへのアクセスを行う。

【0012】

ここで、あるデバイスファイルに対するアクセスについての規則（以下、アクセス規則とも記す）は、ディレクトリごとに決められる。

図1に示すように、例えば、ディレクトリ”a／b”に対しては、デバイスファイルへのアクセスは、読み出し（read）のみが許可されるアクセス規則が設定される。

また、例えば、ディレクトリ”a／c”に対しては、デバイスファイルへのアクセスは、読み出しおよび書き込み（read・write）の両方が許可されるアクセス規則が設定される。

なお、実際には、例えば、ディレクトリaに対しては、”root”、ディレクトリbに対しては”dev”、ディレクトリcに対しては”tmp”などの名称が付される。

【0013】

このような場合、同じデバイスファイルにアクセスするのにもかかわらず、あるプロセスが、ディレクトリ”a／b”にある”file#1”を介してデバイスファイルにアクセスするときには、デバイスファイルに対する読み出しのみが許可されるのに対して、ディレクトリ”a／c”にある”file#2”を介してデバイスファイルにアクセスするときには、デバイスファイルに対する読み出しも書き込みも許可されてしまう。

このように、プロセスが、同じデバイスに対してアクセスする場合であっても、プロセスとデバイスファイルとの間でリンクされたファイルやディレクトリ（経路）をどのように選ぶかによって、適用されるアクセス規則が異なることがあると、プロセス処理上の矛盾が生じかねない。

【0014】

[本発明の概要]

図2は、本発明の概要を、具体例を挙げて説明する図である。

なお、図2においては、デバイスが2つ、デバイスファイルが2つ、デバイスファイルにリンクされたファイルが2つ示されているが、これらの数は例示であり、また、ディレクトリも例示である。

従って、本発明に係るアクセス制御方法は、これらの数およびディレクトリ構成に限定されない。

また、図2に示されたアクセス規則は例示であって、本発明に係るアクセス制御方法は、この規則に限定されることはない。

【0015】

このように、アクセス規則に生じる可能性がある不一致・矛盾を解決するためには、プロセス（1つとは限らない）が、同じデバイスにアクセスするときの経路それぞれにデバイスファイルを置き、これら複数のデバイスファイルに対するアクセス規則を統一すればよい。

具体的には、例えば、まず、図2に示すように、あるプロセスからデバイスにアクセスするための経路が複数あるときには、これらの経路それぞれにデバイスファイル（デバイスファイル#1, #2）を置く。

【0016】

次に、これらのデバイスファイル#1, #2それぞれにアクセスするファイル（file#1, #2）が存在する全てのディレクトリ（ディレクトリ”a/b”, ”a/c”）から、デバイスファイル#1, #2にアクセスするためのアクセス規則が、ディレクトリ”a/b”, ”a/c”の間で異なっているときには、これらのアクセス規則を統一し、例えば、書き込み（write）を禁止し、読み出し（read）のみを許可する。

統一されたアクセス規則に従って、デバイスファイルに対するアクセスを行うことにより、ディレクトリ間のアクセス規則の不一致・矛盾が解消され、プロセス処理上の不具合が予防され、また、OSの脆弱性を減ずることができる。

【0017】

なお、ディレクトリ間のアクセス規則は、例えば、OSのセキュリティを向上させるためには、図2に示したように、統一されたアクセス規則として、最も制

限が厳しいものを採用すればよい。

あるいは、例えば、OSのパフォーマンスを向上させるためには、統一されたアクセス規則として、複数の経路の内、最も頻繁に用いられる経路のアクセス規則を採用すればよい。

あるいは、例えば、読み出し動作以外意味のないデバイスなど、デバイスに特徴がある場合、あるいは、経路に含まれるファイルに特徴があるときには、統一されたアクセス規則として、このファイルを含む経路によりデバイスにアクセスするために最適なアクセス規則を採用すればよい。

【0018】

[第1実施形態]

以下、本発明の第1の実施形態を説明する。

【0019】

[コンピュータ1]

図3は、本発明に係るアクセス制御方法が適応されるコンピュータ1のハードウェア構成を例示する図である。

図3に示すように、コンピュータ1は、CPU102、メモリ104およびこれらの周辺回路などを含む本体100、表示装置、キーボードおよびマウスなどを含む表示・入力装置106、ネットワークを介して他のコンピュータなど（いずれも図示せず）との通信を行う通信装置110、HD装置およびCD装置などの記録装置112、および、記録装置112に対して着脱可能な記録媒体114から構成される。

つまり、コンピュータ1は、一般的なコンピュータとしての構成部分を有している。

なお、コンピュータ1の内、本体100内に収容されたインターフェース、表示・入力装置106、通信装置110および記録装置112などが、図1、図2に示したアクセスの対象となるデバイスに相当する。

【0020】

[OS2・第1のユーティリティプログラム30]

図4は、図3に示したコンピュータ1上で動作するOS2の構成と、本発明に

係るアクセス制御方法を実現する第1のユーティリティプログラム30の構成を示す図である。

図4に示すように、OS2は、デバイスドライバ202-1～202-n (n ≥ 1)、ファイルシステム204、デバイスデータベース(デバイスDB)206、デバイスファイルDB208、ディレクトリ管理部210、アクセス制御部212、規則DB214およびプロセス実行部216などから構成される。

また、第1のユーティリティプログラム30は、デバイス番号生成部300、検索部302、規則抽出部304および規則導出部306などから構成される。

【0021】

なお、図4中に点線で示すように、OS2の規則DB214は、ユーティリティプログラム30側に設けられていてもよい。

また、OS2の構成部分の分け方は例示であって、例えば、ファイルシステム204内に、デバイスDB206などのデータベースが作成されてもよい。

また、以下、「デバイスドライバ202-1～202-n」など、複数あり得る構成部分のいずれかを特定せずに示すときには、単に、「デバイスドライバ202」などとも記す。

【0022】

OS2およびユーティリティプログラム30は、例えば、記録媒体114(図3)を介してコンピュータ1に供給され、実行される。

OS2は、これらの構成部分により、プロセス200-1～200-m (m ≥ 1)を実行し、ユーティリティプログラム30から設定されるアクセス規則に従って、図3に示した表示・入力装置106などのデバイスに対するアクセスを制御する。

また、ユーティリティプログラム30は、図2を参照して説明したように、同一のデバイスに対して複数の経路からアクセスがあるときに、この経路ごとに作成されたデバイスファイル(図2)それぞれに対するアクセス規則を統一し、OS2に設定する。

【0023】

OS2において、デバイスドライバ202は、デバイスファイルを介してプロ

セス 200 のアクセスを受け、表示・入力装置 106 などのデバイスを動作させる。

ファイルシステム 204 は、ディレクトリごとにファイル（デバイスファイルを含む）を記憶し、管理する。

デバイス DB 206 は、デバイスと、そのデバイス番号とを対応付けて記憶し、管理する。

【0024】

デバイスファイル DB 208 は、デバイスファイルと、デバイス番号とを対応付けて記憶し、管理する。

ディレクトリ管理部 210 は、ファイルシステム 204 内のディレクトリを管理する。

【0025】

規則 DB 214 は、ファイルシステム 204 内のディレクトリそれぞれに設定されるデバイスファイルへのアクセス規則の設定を受け、設定されたアクセス規則を記憶し、管理する。

規則 DB 214 に設定されるアクセス規則は、上述のように、デバイスファイルに対するアクセスが、読み出しのみについて許可されているか、書き込みのみについて許可されているか、これらの両方について許可されているか、あるいは、これらの両方について禁止されているかを、ファイルシステム 204 内のディレクトリあるいはデバイスファイルごとに規定する。

なお、規則 DB 214 に対しては、コンピュータ 1 の表示・入力装置 106（図 3）に対するユーザの設定操作により、あるいは、ユーティリティプログラム 30 からの通知により、アクセス規則が設定される。

【0026】

アクセス制御部 212 は、規則 DB 214 に記憶されているアクセス規則に従って、プロセス 200 からデバイスファイルへのアクセス、および、プロセス 200 とデバイスファイルとの間の経路にあり、デバイスファイルとリンクされたファイルからデバイスファイルへのアクセスを制御する。

プロセス実行部 216 は、プロセス 200 を実行する。

【0027】

ユーティリティプログラム30において、検索部302は、デバイスファイルDB208を検索し、デバイスファイルと、そのデバイスファイルに対応するデバイスのデバイス番号などを示す情報を得る。

デバイス番号生成部300は、デバイスファイルDB208に対する検索の結果として得られた情報を解析し、デバイスファイルに対応するデバイスのデバイス番号を生成する。

規則抽出部304は、規則DB214を検索し、デバイスファイルそれぞれに対するアクセスについて、ディレクトリあるいはデバイスファイルごとに設定されたアクセス規則を抽出する。

【0028】

規則導出部306は、抽出されたアクセス規則の内、同じデバイスファイルに対する複数のディレクトリからのアクセスについて設定されたアクセス規則を、例えば、上述したように、最もデバイスファイルに対するアクセスの条件が厳しくなるように統一するように、アクセス規則を導出する。

また、あるいは、規則導出部306は、複数のアクセス規則のいずれかに、全てのアクセス規則を統一するように、アクセス規則を導出する。

あるいは、規則導出部306は、デバイスファイルにリンクされたファイルの性質に応じて統一するように、アクセス規則を導出する。

このように、規則導出部306は、同一のデバイスに対する複数のデバイスファイルに対する各ディレクトリのアクセス規則が統一されるように、各デバイスごとにアクセス規則を導出し、OS2の規則DB214に記憶させる。

【0029】

【第1のユーティリティプログラム30の動作】

図5は、図4に示した第1のユーティリティプログラム30の動作(S10)を示すフローチャートである。

OS2側でデバイスファイルに対するアクセスが生じると、OS2のアクセス制御部212が、第1のユーティリティプログラム30に対して、アクセスされたデバイスファイルを示す情報を含むアクセス規則導出依頼を発行する。

図5に示すように、ステップ100（S100）において、ユーティリティプログラム30は、OS2からアクセス規則導出依頼が来たか否かを判断する。

ユーティリティプログラム30は、アクセス規則導出依頼が来たときにはS102の処理に進み、これ以外のときにはS100の処理に留まる。

【0030】

ステップ102（S102）において、検索部302は、OS2のデバイスファイルDB208を検索し、全てのデバイスファイルの情報を得る。

デバイス番号生成部300は、検索の結果として得られたデバイスファイルの情報それぞれから、デバイスファイルに対応するデバイスのデバイス番号を取り出す。

【0031】

ステップ104（S104）において、規則抽出部304は、取り出されたデバイス番号から、アクセスされたデバイスファイルに対応するデバイスのデバイス番号と同じデバイス番号を検索する。

ステップ106（S106）において、規則抽出部304は、検索の結果として、アクセスされたデバイスファイルに対応するデバイスのデバイス番号と同じデバイス番号が複数、見つかったか否かを判断する。

ユーティリティプログラム30は、検索の結果として同じデバイス番号が複数あったときにはS108の処理に進み、これ以外のときにはS114の処理に進む。

【0032】

ステップ108（S108）において、規則抽出部304は、OS2の規則DB214を検索し、S106の処理において複数、見つかったデバイス番号のデバイスにアクセスする全てのデバイスファイルに対して設定されたアクセス規則の情報を得る。

規則抽出部304は、検索の結果として見つかった情報からアクセス規則を抽出する。

【0033】

ステップ110（S110）において、規則導出部306は、抽出されたア

セス規則を統一するアクセス規則を導出する。

つまり、規則導出部306は、上記デバイス番号のデバイスに対応する複数のデバイスファイルにリンクされた複数のファイルを含む複数のディレクトリそれぞれに対して設定されるアクセス規則を統一する。

【0034】

ステップ112（S112）において、規則導出部306は、導出されたアクセス規則をOS2に通知する。

S112の処理による通知を受けたOS2の規則DB214は、通知に従ってアクセス規則を変更し、アクセス制御部212は、変更されたアクセス規則に従って、デバイスファイルに対するアクセスを制御する。

ステップ114（S114）において、規則導出部306は、アクセス規則の変更がない旨をOS2に通知する。

この場合は、OS2の規則DB214は、アクセス規則を変更しない。

【0035】

[OS2の動作]

次に、OS2のアクセス制御に関する動作を説明する。

図6は、図4に示したOS2のアクセス制御に関する動作（S12）を示す図である。

図6に示すように、ステップ120（S120）において、OS2のアクセス制御部212は、プロセス200あるいはデバイスファイルにリンクされたファイルが、デバイスファイルに対するアクセスのために、ファイルオープンを要求したか否かを判断する。

OS2は、ファイルオープンの要求があったときにはS122の処理に進み、これ以外のときにはS120の処理に留まる。

【0036】

ステップ122（S122）において、アクセス制御部212は、ユーティリティプログラム30に対してアクセス規則導出依頼を発行する。

このアクセス規則導出依頼を受けると、ユーティリティプログラム30は、図5に示した処理を実行する。

ステップ124 (S124)において、規則DB214は、ユーティリティープログラム30から、アクセス規則の通知 (S112, S114; 図5)を受けたか否かを判断する。

OS2は、アクセス規則の通知を受けたときにはS126の処理に進み、これ以外のときにはS124の処理に留まる。

【0037】

ステップ126 (S126)において、規則DB214は、ユーティリティープログラム30からの通知が、アクセス規則の変更があることを示しているか否かを判断する。

OS2は、ユーティリティープログラム30からの通知がアクセス規則の変更があることを示しているときにはS128の処理に進み、これ以外のときにはS130の処理に進む。

ステップ128 (S128)において、規則DB214は、ユーティリティープログラム30からの通知に従って、アクセス規則を変更して記憶・管理する。

【0038】

ステップ130 (S130)において、アクセス制御部212は、デバイスファイルに対するアクセスが、規則DB214に記憶されているアクセス規則に適合するか否かを判断する。

OS2は、デバイスファイルへのアクセスがアクセス規則に適合している場合にはS132の処理に進み、これ以外の場合にはS134の処理に進む。

【0039】

ステップ132 (S132)において、アクセス制御部212は、デバイスファイルのファイルオープンのための処理を行う。

ステップ134 (S134)において、アクセス制御部212は、デバイスファイルに対するアクセスを拒否する。

【0040】

[全体動作]

以下、OS2およびユーティリティープログラム30の全体的な動作を説明する。

図7は、図4に示したOS2および第1のユーティリティープログラム30の全

体的な動作（S14）を示すシーケンス図である。

図7に示すように、ステップ140（S140）において、プロセス200は、直接、あるいは、ファイルを介して、OS2に対してデバイスファイルのファイルオープンを要求する。

【0041】

ステップ142（S142）において、OS2は、ユーティリティプログラム30に対して、規則導出を依頼する。

ステップ146（S146）において、ユーティリティプログラム30は、OS2に対して、デバイスファイルの検索など、アクセス規則の導出に必要な処理を行う。

【0042】

ステップ148（S148）において、ユーティリティプログラム30は、アクセス規則を導出すると、導出した規則をOS2に通知する。

ステップ150（S150）において、OS2は、ユーティリティプログラム30から通知された規則に従って、デバイスファイルに対するアクセスを許可し、あるいは、不許可にする。

【0043】

[第2実施形態]

以下、本発明の第2の実施形態を説明する。

第1の実施形態として、デバイスファイルへのアクセスが生じるたびに、OS2から第1のユーティリティプログラム30に対して規則導出を依頼する方法を説明した。

しかしながら、この方法によると、デバイスファイルへのアクセスが発生するたびに、ユーティリティプログラム30によるアクセス規則の導出が行われるので、デバイスファイルにアクセスするために時間がかかり、また、処理付加も大きい。

本発明の第2の実施形態は、このような点を解決するために、OS2の起動時に、全体的なアクセス規則の導出を行い、その後は、OS2のアクセス規則の変更が生じたときに、第2のユーティリティプログラム32（図8を参照して後述

) によるアクセス規則の導出を行うように改良されている。

【0044】

図8は、第2のユーティリティプログラム32の構成を示す図である。

なお、図8に示した第2のユーティリティプログラム32の構成部分の内、図4に示したユーティリティプログラム30の構成部分と実質的に同じものには、同じ符号が付されている。

図8に示すように、第2のユーティリティプログラム32は、第1のユーティリティプログラム30(図4)に、差分規則導出部320を付加した構成を採る。

【0045】

第2のユーティリティプログラム32も、第1のユーティリティプログラム30と同様に、記録媒体114などを介してコンピュータ1に供給され、実行される。

差分規則導出部320は、OS2からアクセス規則導出依頼を受けたときに、アクセス規則が変更されたアクセスファイル(差分)について、アクセス規則の導出を行う。

【0046】

[OS2および第2のユーティリティプログラム32の動作]

以下、第2の実施形態におけるOS2および第2のユーティリティプログラム32の動作を説明する。

図9は、第2のユーティリティプログラム32起動時の動作(S16)を示すフローチャートである。

なお、図9に示した各処理の内、図5に示した処理と実質的に同じものには同じ符号が付されている(以下の各図について同じ)。

OS2が起動されると、OS2は、ユーティリティプログラム32を起動する。

【0047】

図9に示すように、ステップ160(S160)において、ユーティリティプログラム32の検索部302は、OS2の規則DB214に記憶されている全て

のアクセス規則、および、デバイスファイルDB208に記憶されている全てのデバイスファイルを取得する。

ステップ162（S162）において、デバイス番号生成部300は、S160の処理において得られたデバイスファイルの情報からデバイス番号を抽出する。

【0048】

ステップ164（S164）において、規則抽出部304は、S162の処理により得られたデバイス番号に基づいて、デバイスそれぞれに対応するデバイスファイルを抽出する。

ステップ166（S166）において、規則抽出部304は、共通のデバイスに対応して複数のデバイスファイルが設けられているか、つまり、規則導出の対象となるデバイスがあるか否かを判断する。

【0049】

ユーティリティプログラム32は、規則導出の対象となるデバイスがある場合にはS108の処理に進み、これ以外の場合にはS114の処理に進む。

S108～S114（図5を参照）の処理において、ユーティリティプログラム32は、アクセス規則の導出およびOS2に対する規則の通知を行う。

【0050】

図10は、図9に示した第2のユーティリティプログラム32の処理により規則の通知を受けたOS2の動作（S18）を示すフローチャートである。

ステップ180（S180）において、OS2の規則DB214は、ユーティリティプログラム32からの規則を受信する。

ステップ182（S132）において、規則DB214は、ユーティリティプログラム32の通知に従って、アクセス規則を変更して記憶・管理する。

これ以降、アクセス制御部212は、規則DB214に記憶・管理されたアクセス規則に従ってアクセス制御を行う。

【0051】

図11は、アクセス規則の変更に関するOS2の動作（S20）を示すフローチャートである。

図12は、OS2によるアクセス制御の動作(S22)を示すフローチャートである。

図11に示すように、規則DB214は、アクセス規則を変更する設定がなされたか否かを判断する。

OS2は、アクセス規則を変更する設定がなされたときにはS202の処理に進み、これ以外の場合にはS200の処理に留まる。

なお、アクセス規則が変更される場合には、上述のように、規則DB214に対する設定変更の他に、アクセス制御部212によるディレクトリ構成の変更、あるいは、デバイスDB206に対するデバイス設定の変更なども含まれる。

【0052】

ステップ202(S202)において、アクセス制御部212は、ユーティリティプログラム32に対して、アクセス規則が変更されたデバイスファイルについての情報(差分情報；アクセス規則が変更されたデバイスファイルおよびそれに対応するデバイスのデバイス番号など)を含むアクセス規則変更依頼を発行する。

このアクセス規則変更依頼を受けると、ユーティリティプログラム32は、差分についてのアクセス規則の導出(図13を参照して後述)を行い、OS2に対して導出結果を通知する。

S124～S128の処理(図6)において、規則DB214は、ユーティリティプログラム32からのアクセス規則の通知に従って、アクセス規則を変更し、あるいは、変更しないまととする。

アクセス制御部212は、図12に示すS120, S130, S132(図6)の処理において、以上のように変更され、あるいは変更されないまとされたアクセス規則に従って、アクセス制御を行う。

【0053】

図13は、図11に示したOS2の処理(S20)により、アクセス規則の導出依頼を受けた第2のユーティリティプログラム32の処理(S24)を示すフローチャートである。

図13に示すように、ステップ240(S240)において、ユーティリティ

プログラム 32 は、OS2 からのアクセス規則導出依頼を受けたか否かを判断する。

ユーティリティプログラム 32 は、アクセス導出依頼を受けた場合には S242 の処理に進み、これ以外の場合には S240 の処理に留まる。

【0054】

ステップ 242 (S242) において、デバイス番号生成部 300 は、OS2 から受けた差分情報からデバイス番号を取り出す。

ステップ 244 (S244) において、S242 の処理により取り出されたデバイス番号に、同一のデバイス番号が複数あるいか否かを判断する。

ユーティリティプログラム 32 は、同一のデバイス番号が複数あるときには S246 の処理に進み、これ以外のときには S250 の処理に進む。

【0055】

ステップ 246 (S246) において、差分検出部 320 は、アクセス規則が変更されたデバイスファイル（差分）に対応するデバイスについて、統一のアクセス規則を導出する。

ステップ 248 (S248) において、差分規則導出部 320 は、差分について導出したアクセス規則を OS2 に対して通知する。

ステップ 250 (S250) において、差分規則導出部 320 は、差分についてアクセス規則が変更されない旨を OS2 に通知する。

【0056】

[OS2 および第2のユーティリティプログラム 32 の全体動作]

以下、OS2 および第2のユーティリティプログラム 32 の全体的な動作を説明する。

図 14 は、OS2 およびユーティリティプログラム 32 (図 8) の起動時の全体的な動作 (S26) を示すフローチャートである。

OS2 が起動されると、図 14 に示すように、ステップ 260 (S260) において、OS2 は、ユーティリティプログラム 32 を起動する。

【0057】

ステップ 262 (S262) において、ユーティリティプログラム 32 は、規

則DB214およびデバイスファイルDB208を検索し、アクセス規則導出に必要な情報を取得する。

ステップ264(S264)において、ユーティリティプログラム32は、OS2に対して、導出したアクセス規則を通知する。

【0058】

図15は、アクセス規則に変更が生じたときのOS2およびユーティリティプログラム32(図8)の全体的な動作(S28)を示すフローチャートである。

アクセス規則の変更が生じると、図15に示すように、ステップ280(S280)において、OS2は、ユーティリティプログラム32に対して、差分情報を含むアクセス規則導出依頼を発行する。

ユーティリティプログラム32は、このアクセス規則導出依頼を受けて、図13に示したように、差分についてアクセス規則を導出する。

ステップ282(S282)において、ユーティリティプログラム32は、差分について導出されたアクセス規則をOS2に通知する。

【0059】

【発明の効果】

以上説明したように、本発明に係るアクセス制御システムおよびその方法によれば、コンピュータのOSの脆弱性を手当てして、その安全性を向上させることができる。

【図面の簡単な説明】

【図1】

本発明の背景を、具体例を挙げて説明する図である。

【図2】

本発明の概要を、具体例を挙げて説明する図である。

【図3】

本発明に係るアクセス制御方法が適応されるコンピュータのハードウェア構成を例示する図である。

【図4】

図3に示したコンピュータ上で動作するOSの構成と、本発明に係るアクセス

制御方法を実現する第1のユーティリティプログラムの構成を示す図である。

【図5】

図4に示した第1のユーティリティプログラムの動作(S10)を示すフローチャートである。

【図6】

図4に示したOSのアクセス制御に関する動作(S12)を示す図である。

【図7】

図4に示したOSおよび第1のユーティリティプログラムの全体的な動作(S14)を示すシーケンス図である。

【図8】

第2のユーティリティプログラムの構成を示す図である。

【図9】

第2のユーティリティプログラムの起動時の動作(S16)を示すフローチャートである。

【図10】

図9に示した第2のユーティリティプログラムの処理により規則の通知を受けたOSの動作(S18)を示すフローチャートである。

【図11】

アクセス規則の変更に関するOSの動作(S20)を示すフローチャートである。

【図12】

OSによるアクセス制御の動作(S22)を示すフローチャートである。

【図13】

図11に示したOSの処理(S20)により、アクセス規則の導出依頼を受けた第2のユーティリティプログラムの処理(S24)を示すフローチャートである。

【図14】

OSおよびユーティリティプログラム(図8)の起動時の全体的な動作(S26)を示すフローチャートである。

【図15】

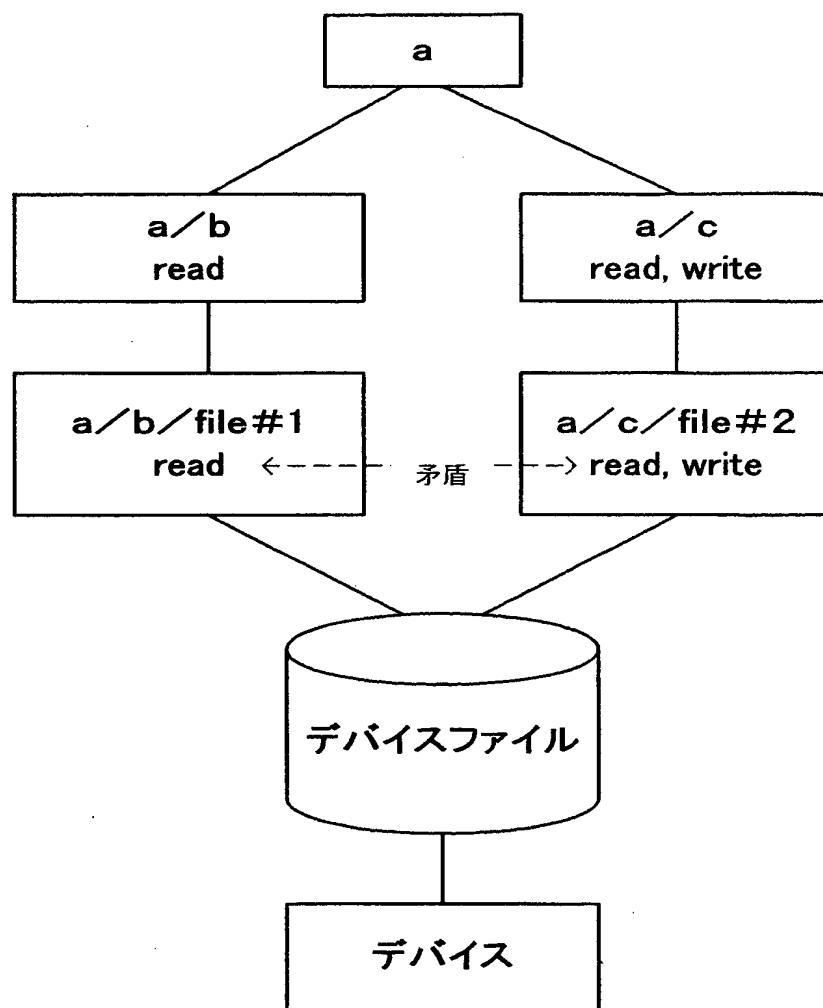
アクセス規則に変更が生じたときのOSおよびユーティリティプログラム（図8）の全体的な動作（S28）を示すフローチャートである。

【符号の説明】

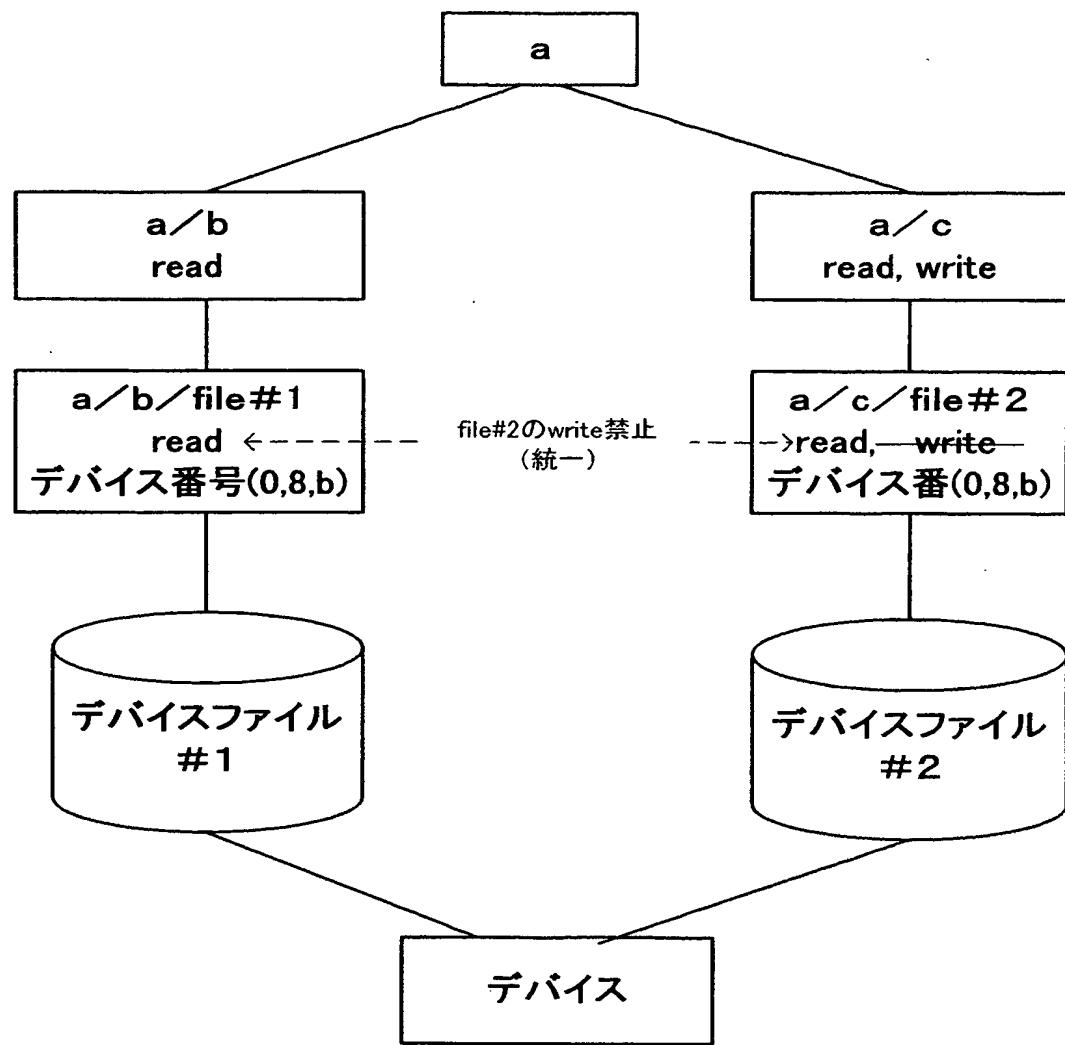
1 . . . コンピュータ、
100 . . . 本体、
102 . . . CPU、
104 . . . メモリ、
106 . . . 表示・入力装置、
110 . . . 通信装置、
112 . . . 記録装置、
114 . . . 記録媒体、
2 . . . OS、
200 . . . プロセス、
202 . . . デバイスドライバ、
204 . . . ファイルシステム、
206 . . . デバイスDB、
208 . . . デバイスファイルDB、
210 . . . ディレクトリ管理部、
212 . . . アクセス制御部、
214 . . . 規則DB、
216 . . . プロセス実行部、
30, 32 . . . ユーティリティプログラム、
300 . . . デバイス番号生成部、
302 . . . 検索部、
304 . . . 規則抽出部、
306 . . . 規則導出部、
308 . . . 規則DB、
320 . . . 差分規則導出部、

【書類名】 図面

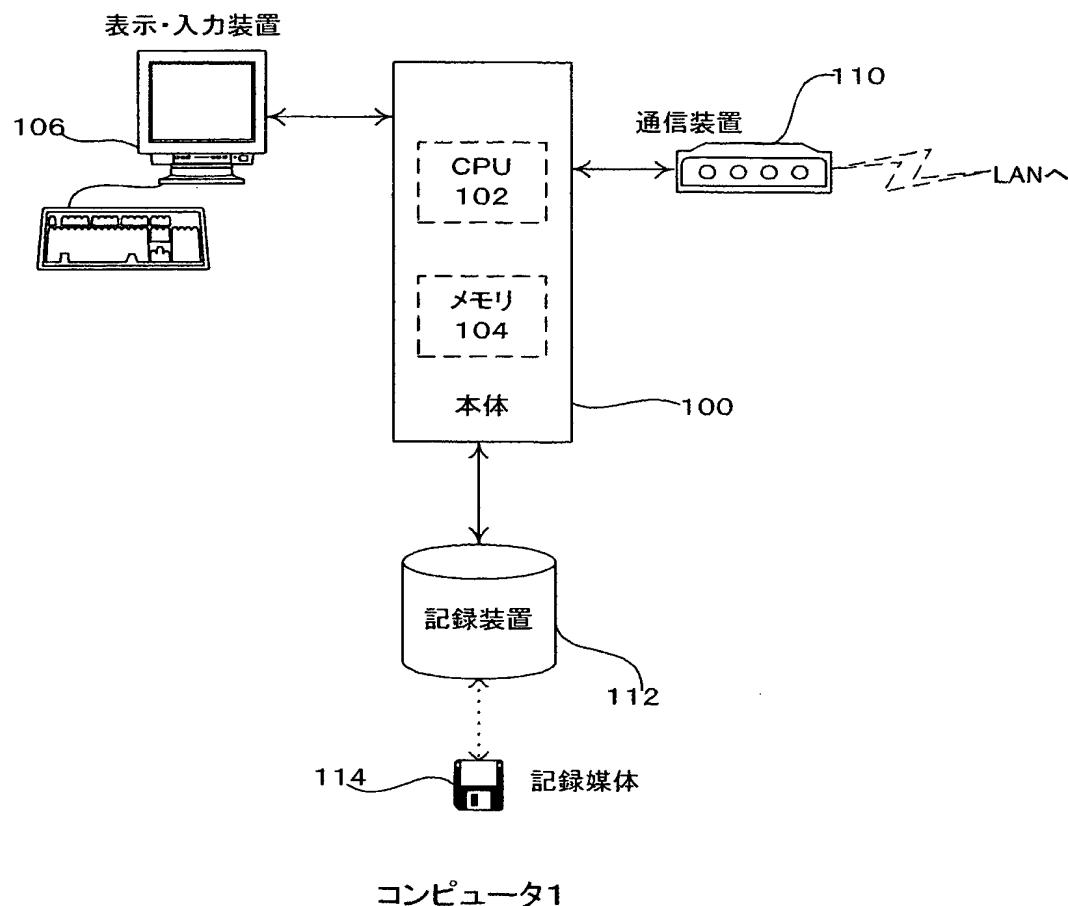
【図 1】



【図2】

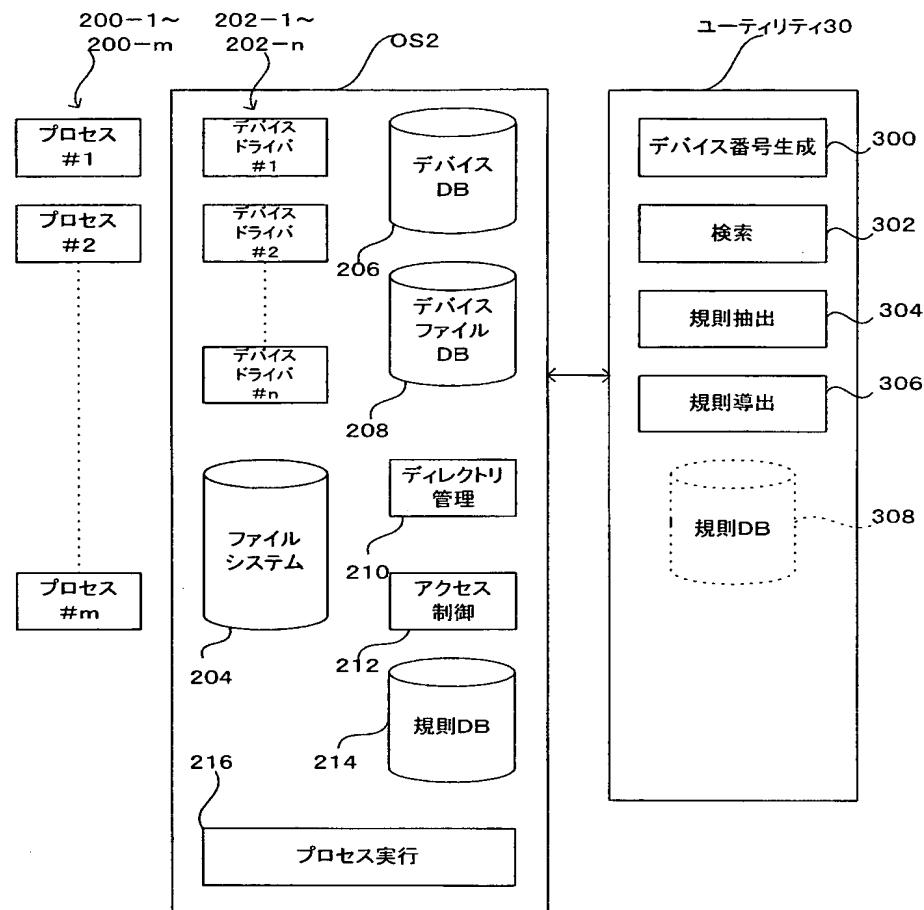


【図3】

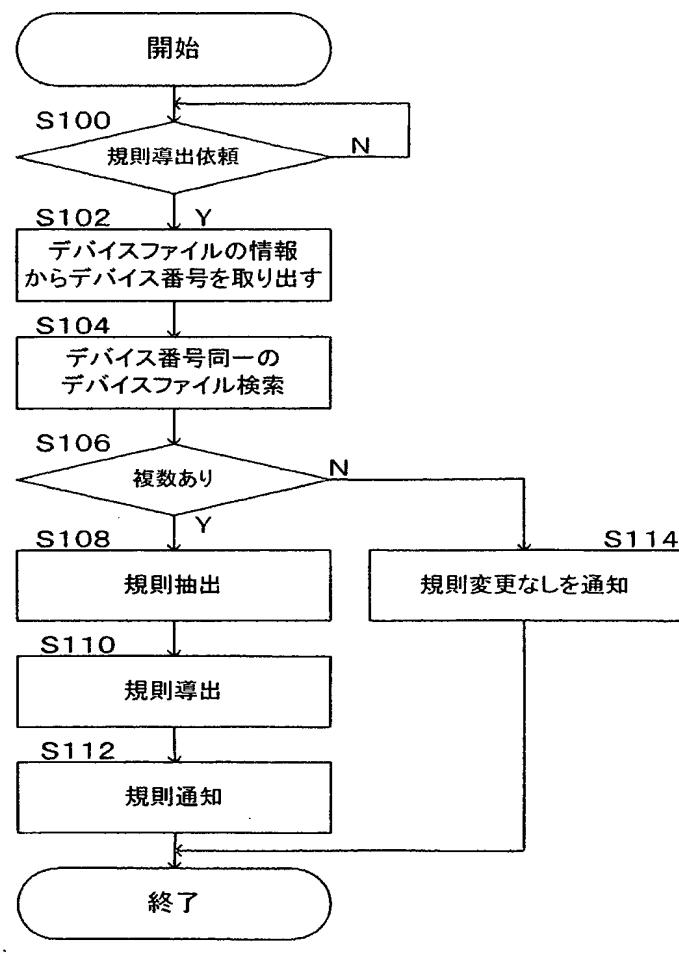


コンピュータ1

【図 4】

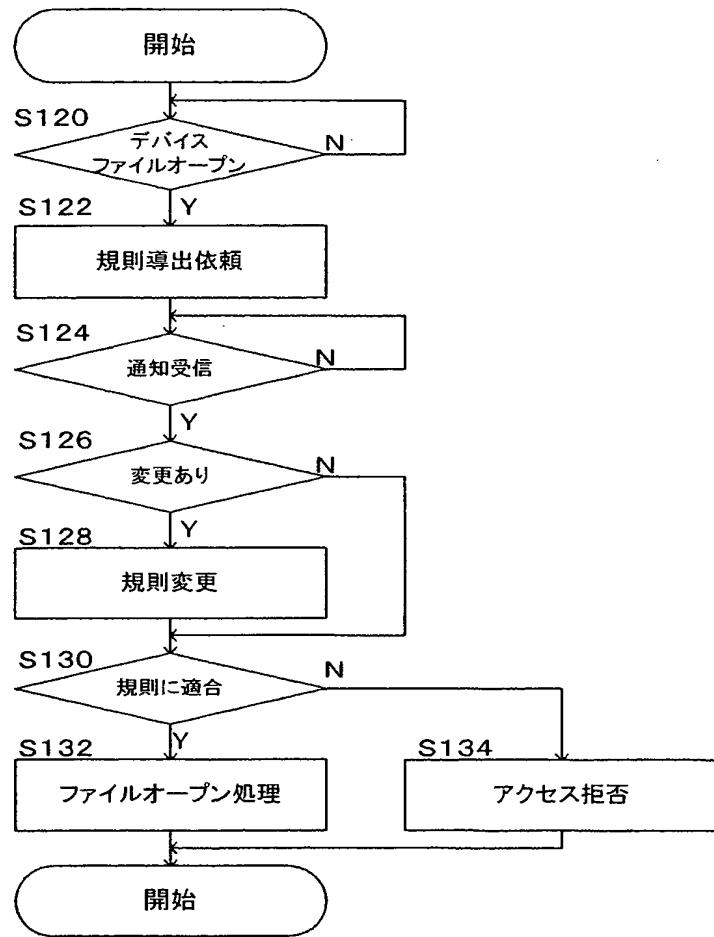


【図 5】



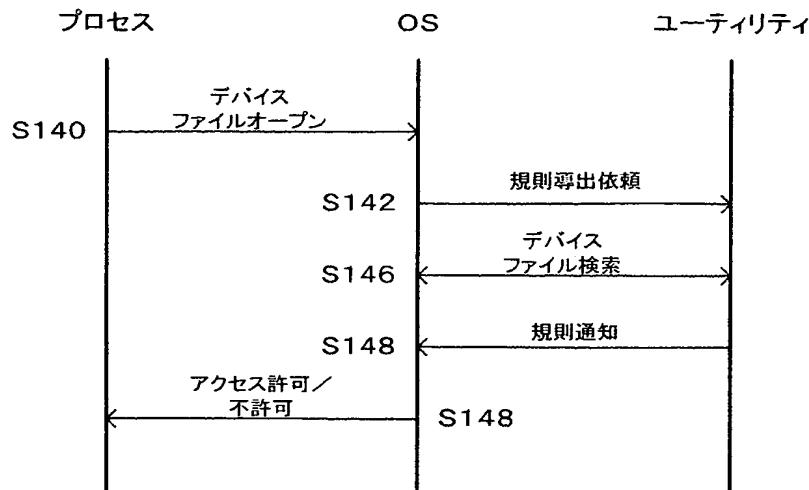
S10

【図 6】



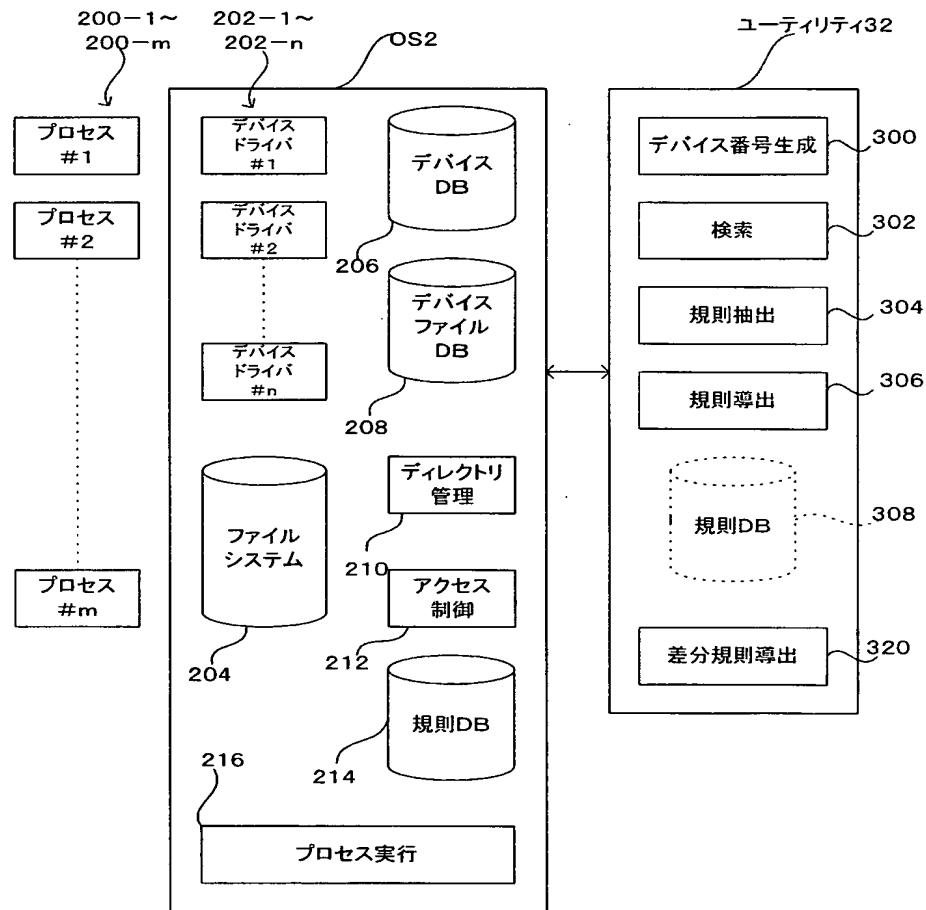
S12

【図 7】

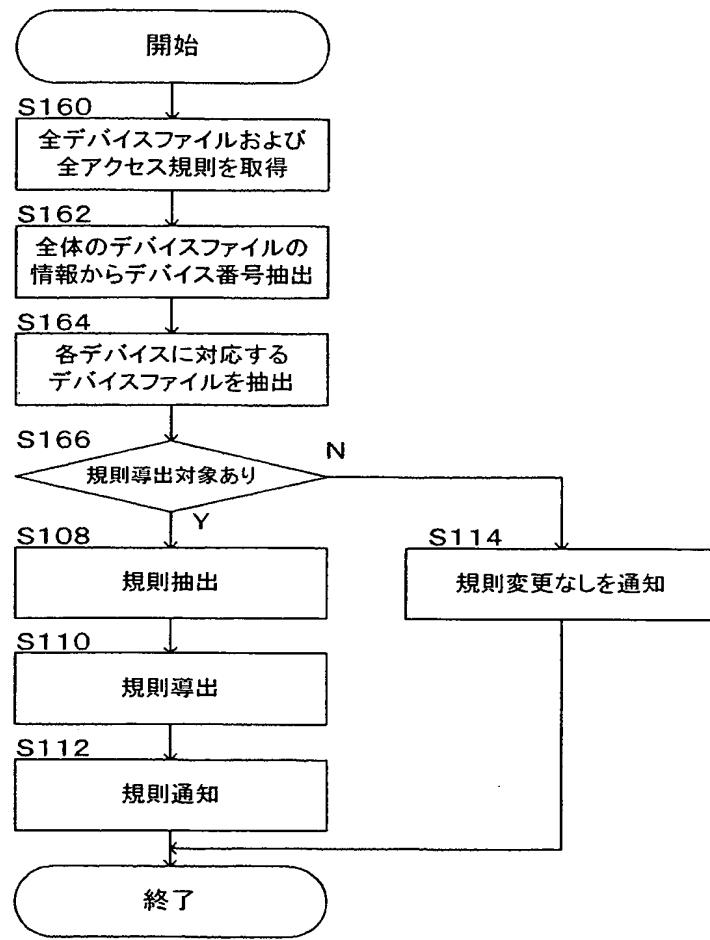


S14

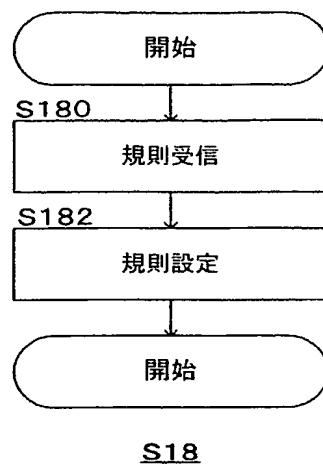
【図8】



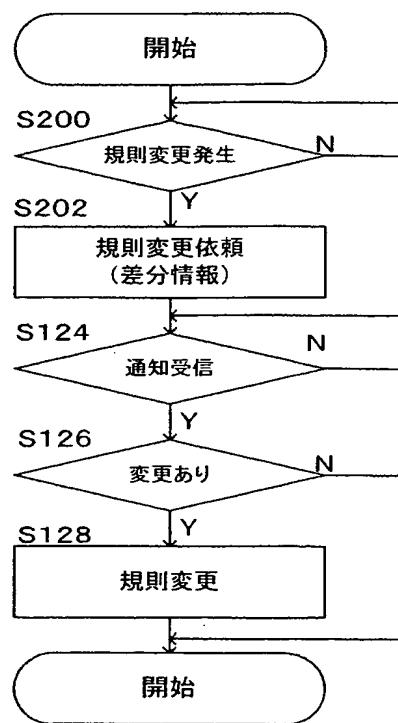
【図9】

S16

【図10】

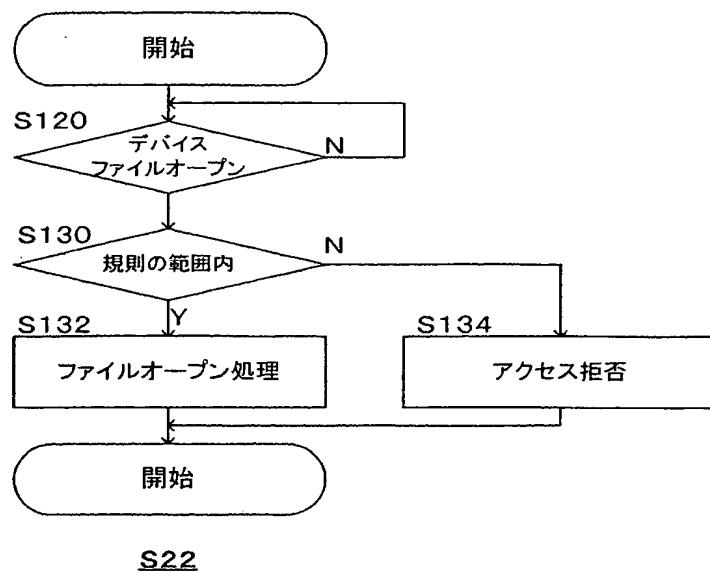


【図 1 1】

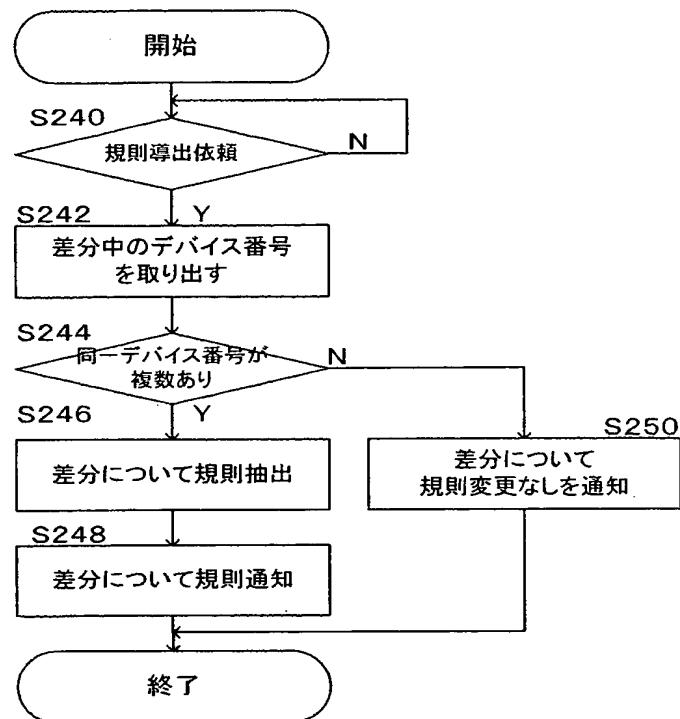


S20

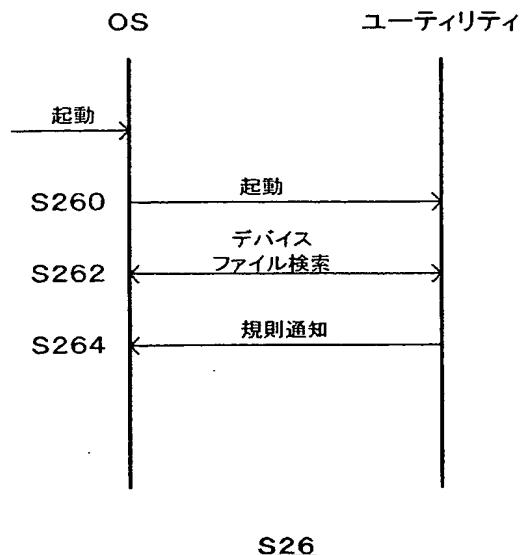
【図12】

S22

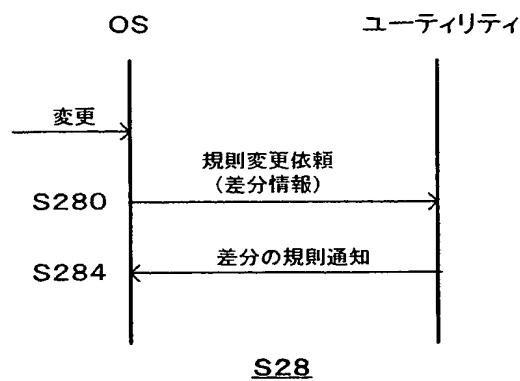
【図13】

S24

【図 1 4】

S26

【図 1 5】

S28

【書類名】 要約書

【要約】

【課題】 コンピュータのOSの脆弱性を手当てして、その安全性を向上させる。

【解決手段】 プロセスが、同じデバイスにアクセスするときの経路それぞれにデバイスファイルを置き、これら複数のデバイスファイルに対するアクセス規則を統一する。例えば、あるプロセスからデバイスにアクセスするための経路が2つあるときには、これらの経路それぞれにデバイスファイル#1, #2を置く。これらのデバイスファイルにアクセスする全てのディレクトリ（a/b, a/c）に対して設定されるアクセス規則を読み出し（read）のみに統一し、2つの経路のいずれからも、同じ規則に従って、デバイスファイルがアクセスされるようとする。

【選択図】 図2

特願 2003-104756

出願人履歴情報

識別番号 [399117110]

1. 変更年月日 1999年10月13日

[変更理由] 新規登録

住 所 東京都杉並区高井戸東3丁目29番21号

氏 名 日本ヒューレット・パッカード株式会社